

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Fumihikko SANO

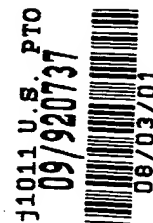
GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: ENCRYPTION/DECRYPTION APPARATUS, AUTHENTICATING APPARATUS, PROGRAM AND METHOD



REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

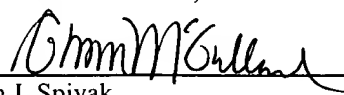
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-237268	August 4, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and  
(B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland  
Registration Number 21,124



22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 10/98)

日 本 国 特 許 庁

JAPAN PATENT OFFICE

Best Available Copy

J1011 U.S.  
09/92073  
08/03/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 8月 4日

出 願 番 号

Application Number:

特願2000-237268

出 願 人

Applicant(s):

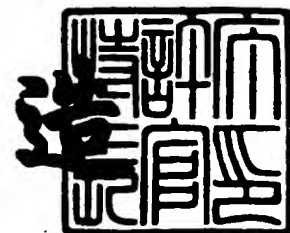
株式会社東芝

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 6月27日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3060496

【書類名】 特許願

【整理番号】 A009904721

【提出日】 平成12年 8月 4日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明の名称】 暗復号装置、認証装置及び記憶媒体

【請求項の数】 8

【発明者】

【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中事業所内

【氏名】 佐野 文彦

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗復号装置、認証装置及び記憶媒体

【特許請求の範囲】

【請求項 1】 互いに並列に設けられ、鍵データに基づいて平文データをブロック毎に暗号化して暗号文データを出力し、及び／又は鍵データに基づいて暗号文データをブロック毎に復号して平文データを出力する複数の暗号化関数部と

いずれかの暗号化関数部の中間的な処理結果に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成手段とを備えた暗復号装置であって、

前記各鍵データ生成手段は、互いに異なる 2 つ以上の変換処理のうち、いずれかの変換処理を用いて前記共通鍵を変換することを特徴とする暗復号装置。

【請求項 2】 請求項 1 に記載の暗復号装置において、

前記各鍵データ生成手段は、互いに異なる 2 つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とする暗復号装置。

【請求項 3】 メッセージから認証子を生成する認証子生成手段を備え、前記認証子生成手段により生成された認証子に基づいて前記メッセージの認証を行なう認証装置であって、

前記認証子生成手段は、

互いに並列に設けられ、鍵データに基づいて前記メッセージをブロック毎に暗号化して暗号文データを作成する複数の暗号化関数部と、

いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる 2 つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成部と、

最終段の暗号化関数部により作成された暗号文データに基づいて、前記認証子を作成する認証子作成部と

を備えたことを特徴とする認証装置。

【請求項 4】 請求項 3 に記載の認証装置において、

前記各鍵データ生成部は、互いに異なる 2 つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とする認証装置。

【請求項 5】 暗復号装置のコンピュータを、

互いに並列に設けられ、鍵データに基づいて平文データをブロック毎に暗号化して暗号文データを出力し、及び／又は鍵データに基づいて暗号文データをブロック毎に復号して平文データを出力する複数の暗号化関数部、

いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる 2 つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成手段、

として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項 6】 請求項 5 に記載のコンピュータ読取り可能な記憶媒体において、

前記各鍵データ生成手段は、互いに異なる 2 つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とするコンピュータ読取り可能な記憶媒体。

【請求項 7】 メッセージから認証子を生成し、この認証子に基づいて前記メッセージの認証を行なう認証装置に使用されるコンピュータ読取り可能な記憶媒体であって、

前記認証装置のコンピュータを、

互いに並列に設けられ、鍵データに基づいて前記メッセージをブロック毎に暗号化して暗号文データを作成する複数の暗号化関数部、

いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる 2 つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成部、

最終段の暗号化関数部により作成された暗号文データに基づいて、前記認証子

を作成する認証子作成部、

として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。

【請求項 8】 請求項 7 に記載のコンピュータ読取り可能な記憶媒体において、

前記各鍵データ生成部は、互いに異なる 2 つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換することを特徴とするコンピュータ読取り可能な記憶媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ブロック暗号における暗号化連鎖方式を用いた暗復号装置、認証装置及び記憶媒体に係り、特に、各ブロック間での連鎖のさせ方を全体で 2 種類以上設けて安全性を向上し得る暗復号装置、認証装置及び記憶媒体に関する。

【 0 0 0 2 】

【従来の技術】

近年、計算機や通信技術の分野では、送信データを暗号化して送信し、受信データを復号して受信内容を得る暗号技術が広く知られている。この種の暗号技術では、暗号化と復号に同じ秘密鍵（以下、共通鍵という）を用いる暗号化アルゴリズムが共通鍵暗号方式と呼ばれている。共通鍵暗号方式では、一般に、入力される平文データが固定長の入力ブロックに分割され、各ブロックが共通鍵から生成される鍵に基づいて攪拌処理され、暗号文に変換されている。

【 0 0 0 3 】

ここで、平文データが暗号化アルゴリズムのブロック長よりも長い場合、入力データがブロック長で分割され、暗号化された結果が CBC モード (cipher block chaining mode; 暗号文連鎖モード)、インナー CBC モード (inner CBC mode)、CBCM モード (CBC message mode) といった周知の暗号化連鎖方式により、結合される。

【 0 0 0 4 】

図 7 はこの種の暗号化連鎖方式の適用された暗復号装置の構成を示す模式図である。この暗復号装置では、入力された平文データが一定長の  $m$  個の平文ブロック  $P_1 \sim P_m$  に分割され、各平文ブロック  $P_1 \sim P_m$  が、互いに並列配置された  $m$  個の暗号化関数  $F_1 \sim F_m$  のいずれかに入力される。各暗号化関数  $F_1 \sim F_m$  は、入力された平文ブロック  $P_1 \sim P_m$  を共通鍵  $K$  に基づく鍵データにより暗号化し、それぞれ暗号文ブロック  $C_1 \sim C_m$  に変換して出力する。なお、暗復号装置は、暗号文ブロック  $C_1 \sim C_m$  が入力されると、この暗号文ブロック  $C_1 \sim C_m$  を上記暗号化と逆の処理にて復号し、それぞれ平文ブロック  $P_1 \sim P_m$  に変換して出力する。

## 【 0 0 0 5 】

ここで、1 番目の暗号化関数  $F_1$  は、1 番目の平文ブロック  $P_1$  と共通鍵  $K$  が入力されると、1 番目の中間出力  $i_1$  を 1 番目の変換関数  $f_1$  に入力する一方、暗号文  $C_1$  を出力する。

## 【 0 0 0 6 】

1 番目の変換関数  $f_1$  は、例えば非線形な関数がいられ、暗号化関数  $F_1$  の中間出力  $i_1$  を変換し、得られた変換結果  $s_1$  を 1 番目の変換関数  $g_1$  に入力する。なお、2 番目  $\sim$   $(m-1)$  番目の変換関数  $f_2 \sim f_{m-1}$  も同様である。

## 【 0 0 0 7 】

1 番目の変換関数  $g_1$  は、例えば排他的論理和又は加算といった線形関数がいられ、別途入力された共通鍵  $K$  を、変換関数  $f_1$  の変換結果  $s_1$  により変換し、得られた変換結果  $K g_2$  を 2 番目の暗号化関数  $F_2$  に入力する。また、2 番目  $\sim$   $(m-1)$  番目の変換関数  $g_2 \sim g_{m-1}$  も同様である。

## 【 0 0 0 8 】

以下同様に、共通鍵  $K$  は、 $(n-1)$  番目の暗号化関数  $F_{(n-1)}$  による中間出力  $i_{n-1}$  と、 $(n-1)$  番目の変換関数  $f_{n-1}$ 、 $g_{n-1}$  とに基づいて、鍵データ  $K g_n$  (但し  $2 \leq n \leq m$ ) に変換され、鍵データ  $K g_n$  として  $n$  番目の暗号化関数  $F_n$  に入力される。係る前段の中間出力  $i_{n-1}$  と共通鍵  $K$  から次段の鍵データ  $K g_n$  を生成する処理は、 $m$  番目の暗号化関数  $F_m$  に鍵データ  $K g_m$  を入力するまで行なわれる。なお、各変換関数  $g_1 \sim g_{m-1}$  に入力される共通鍵  $K$  は、1 番目の暗号化関数



F1に入力された共通鍵Kと同一である。

#### 【0009】

係る暗号化連鎖方式では、 $m$ 個の暗号化関数 $F_1 \sim F_m$ に使用される鍵 $K$ 、 $K_{g2} \sim K_{gm}$ が互いに異なるため、高い安全性を有している。

しかしながら、以上のような暗号化連鎖方式では、互いに同一の平文ブロック $P_1 \sim P_m$ が入力された場合、全ての変換関数 $f_1 \sim f_{m-1}$ の変換結果 $s_1 \sim s_{m-1}$ が0となり、共通鍵 $K$ を変換関数 $g_1 \sim g_{m-1}$ で変換した変換結果 $K_{g2} \sim K_{gm}$ と、共通鍵 $K$ とが一致してしまう。

#### 【0010】

なお、各鍵 $K$ 、 $K_{g2} \sim K_{gm}$ が一致した場合、 $m$ 個の暗号化関数 $F_1 \sim F_m$ にて同一の暗号化が実行され、同一の $m$ 個の暗号文ブロック $C_1$ 、 $C_2$ 、 $C_3$ 、 $\dots$ 、 $C_m$ が出力される。この現象は、暗号解読の大きな手がかりとなり、暗号解読手法に対する安全性を低下させてしまう。

#### 【0011】

##### 【発明が解決しようとする課題】

以上説明したように従来暗号化連鎖方式を用いた暗復号装置では、特定パターンの平文ブロック $P_1 \sim P_m$ の入力により、全ての変換関数 $f_1 \sim f_{m-1}$ の出力が0となって共通鍵 $K$ が変換されない場合がある。これを阻止するには、変換関数 $f_1 \sim f_{m-1}$ の出力が0にならないよう、平文ブロック $P_1 \sim P_m$ や鍵 $K_{g2} \sim K_{gm}$ を注意深く検査する必要がある。

#### 【0012】

係る検査は、特定パターンをもつ平文ブロック $P_1 \sim P_m$ の入力を除去する装置などを付加すれば実現可能である。しかしながら、この種の除去装置を付加する解決手法では、暗号化連鎖方式の価格を上昇させると共に、暗号化連鎖方式の規模を増大させてしまう問題が生じる。

#### 【0013】

また、係る除去装置は、暗号強度の向上には寄与しない。すなわち、費用対効果の観点からは、暗号強度を向上し得る他の解決手法が望まれている。

#### 【0014】

本発明は上記実情を考慮してなされたもので、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上し得る暗復号装置、認証装置及び記憶媒体を提供することを目的とする。

## 【 0 0 1 5 】

## 【課題を解決するための手段】

第1の発明は、互いに並列に設けられ、鍵データに基づいて平文データをブロック毎に暗号化して暗号文データを出力し、及び／又は鍵データに基づいて暗号文データをブロック毎に復号して平文データを出力する複数の暗号化関数部と、

いずれかの暗号化関数部の中間的な処理結果に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成手段とを備えた暗復号装置であって、前記各鍵データ生成手段としては、互いに異なる2つ以上の変換処理のうち、いずれかの変換処理を用いて前記共通鍵を変換する暗復号装置である。

## 【 0 0 1 6 】

また、第2の発明は、メッセージから認証子を生成する認証子生成手段を備え、前記認証子生成手段により生成された認証子に基づいて前記メッセージの認証を行なう認証装置であって、前記認証子生成手段としては、互いに並列に設けられ、鍵データに基づいて前記メッセージをブロック毎に暗号化して暗号文データを作成する複数の暗号化関数部と、いずれかの暗号化関数部の中間的な処理結果、及び互いに異なる2つ以上の変換処理のうちのいずれかの変換処理に基づいて共通鍵を変換し、得られた鍵データを処理開始前のいずれかの暗号化関数部に個別に入力する複数の鍵データ生成部と、最終段の暗号化関数部により作成された暗号文データに基づいて、前記認証子を作成する認証子作成部とを備えた認証装置である。

## 【 0 0 1 7 】

ここで、第1の発明における各鍵生成手段、及び／又は第2の発明における各データ生成部は、互いに異なる2つ以上の変数データのうち、いずれかの変数データに基づいて前記共通鍵を変換する構成としてもよい。

## 【 0 0 1 8 】

また、第 1 及び第 2 の発明は、前述した機能を記述したプログラムを記憶したコンピュータ読取り可能な記憶媒体を用い、当該記憶媒体をコンピュータにインストールして実現させてもよい。

【0019】

(作用)

従って、第 1 の発明は以上のような手段を講じたことにより、暗号化連鎖方式に用いられる各鍵データ生成手段が、互いに異なる 2 つ以上の変換処理のうち、いずれかの変換処理を用いて共通鍵を変換する。

【0020】

これにより、共通鍵の変換結果である鍵データが平文データから一義的には決まらなくなるので、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させることができる。

【0021】

また、第 2 の発明は、認証子を作成する際に、第 1 の発明の暗復号装置を用いるので、第 1 の発明の作用を奏する認証技術を実現させることができる。

【0022】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。

(第 1 の実施形態)

図 1 は本発明の第 1 の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図であり、図 7 と同種の要素には同一符号を付してその詳しい説明を省略し、ここでは異なる要素について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

すなわち、本実施形態は、互いに同一の平文ブロック  $P_1 \sim P_m$  が入力されても、異なる鍵データ  $K_{g_2} \sim K_{g_m}$  を生成させ、安全性の向上を図るものであって、具体的には、各変換関数  $g_1 \sim g_{m-1}$  に個別に変数  $v_1 \sim v_{m-1}$  を入力するための変数入力部  $V_1 \sim V_{m-1}$  を設けている。

【0023】

ここで、 $(m-1)$  個の変数入力部  $V_1 \sim V_{m-1}$  は、それぞれ変数  $v_1 \sim v_{m-1}$  を個

別に変換関数  $g_1 \sim g_{m-1}$  に入力する機能をもっている。

各変数  $v_1 \sim v_{m-1}$  は、全体として2種類以上 $\sim(m-1)$ 種類以下の範囲で異なる値が設定可能であり、全体として種類が多いほど、攪拌性向上の観点から好ましい。各変数  $v_1 \sim v_{m-1}$  は、例えば図2に示すように、初期値（例、システム固有の値） $IV$  をレジスタに格納し、同一の変換関数で順次変換することにより、生成可能となっている。

また、変数  $v_1 \sim v_{m-1}$  の種類が例えば3種類の場合、 $v_1 \sim v_{(m-1)/3}$  が第1の値、 $v_{\{(m-1)/3\}+1} \sim v_{(m-1) \cdot 2/3}$  が第2の値、 $v_{\{(m-1) \cdot 2/3\}+1} \sim v_{m-1}$  が第3の値という設定よりも、 $v_1$  が第1の値、 $v_2$  が第2の値、 $v_3$  が第3の値、 $v_4$  が第1の値、 $\dots$  という設定の方が攪拌性向上の観点から好ましい。すなわち、各変数  $v_1 \sim v_{m-1}$  は、 $t$  種類の値を取り得る場合、互いに隣接する任意の  $t$  個の変数（例、 $v_1 \sim v_t$ 、 $v_{t+1} \sim v_{2t}$ 、 $\dots$ 、 $v_{m-t} \sim v_{m-1}$ ）を互いに異なる値とする設定の方が好ましい。

#### 【0024】

なお、各変換関数  $g_1 \sim g_{m-1}$  は、変数入力部  $V_1 \sim V_{m-1}$  から入力された変数  $v_1 \sim v_{m-1}$  と変換関数  $f_1 \sim f_{m-1}$  から入力された変換結果  $s_1 \sim s_{m-1}$  とに基づいて、別途入力された共通鍵  $K$  を変換し、得られた変換結果  $Kg_2 \sim Kg_m$  を次段の暗号化関数  $F_2 \sim F_m$  に入力する機能をもっている。なお、各変換関数  $g_1 \sim g_{m-1}$  における変換機能としては、前述した通り、例えば排他的論理和又は加算の如き、線形関数が用いられている。

#### 【0025】

また、変換関数  $f_1 \sim f_{m-1}$  は、例えば次の変換処理（1） $\sim$ （8）のうち、任意の1種類の変換処理が使用されている。

（1）入力から任意のビット長を切り落として出力するビット切落し処理。

（2）入力のビット長を必要なビット長とするまでダミービットを埋込むパディング処理。なお、ダミービットは、ブランクなどの冗字や0などが使用可能である。

（3）入力のビットを反転させて出力するビット反転処理。

（4）入力のビットを逆順に並べ換えて出力するビット逆順処理。

(5) 入力のビット同士を任意に置換して出力するビット置換処理。

(6) 入力をハッシュ関数で変換したものから任意のビット長を切り落として出力するハッシュ関数（例、SHA-1, MD5等）+ビット切落し処理。

(7) 入力に定数を加算して出力する定数加算処理。

(8) 入力を恒等変換して出力する恒等変換処理。

【0026】

また、係る暗復号装置は、ハードウェア及び／又はソフトウェアにて実現可能なものであり、ソフトウェアにより実現される場合にはその動作を示すプログラムが予め記憶媒体からインストールされている。

【0027】

次に、以上のように構成された暗復号装置の動作を説明する。

いま、暗復号装置では、前述同様に、入力された平文データが一定長の $m$ 個の平文ブロック $P_1 \sim P_m$ に分割され、各平文ブロック $P_1 \sim P_m$ が、互いに並列配置された $m$ 個の暗号化関数 $F_1 \sim F_m$ のいずれかに入力される。

【0028】

また、各暗号化関数 $F_1 \sim F_m$ は、入力された平文ブロック $P_1 \sim P_m$ を共通鍵 $K$ に基づく鍵データにより暗号化し、それぞれ暗号文ブロック $C_1 \sim C_m$ に変換して出力する。

【0029】

例えば1番目の暗号化関数 $F_1$ は、1番目の平文ブロック $P_1$ と共通鍵 $K$ が入力されると、1番目の中間出力 $i_1$ を1番目の変換関数 $f_1$ に入力する一方、暗号文 $C_1$ を出力する。

【0030】

1番目の変換関数 $f_1$ は、暗号化関数 $F_1$ の中間出力 $i_1$ を変換し、得られた変換結果 $s_1$ を1番目の変換関数 $g_1$ に入力する。

ここまでの過程は、鍵データの生成に関し、従来と同様である。

次に、本実施形態では、従来とは異なり、1番目の変数入力部 $V_1$ が1番目の変数 $v_1$ を1番目の変換関数 $g_1$ に入力する。

【0031】

これにより、1番目の変換関数  $g_1$  は、変数入力部  $V_1$  からの変数  $v_1$  と変換関数  $f_1$  からの変換結果  $s_1$  とに基づいて、別途入力された共通鍵  $K$  を変換し、得られた変換結果  $K g_2$  を次段の暗号化関数  $F_2$  に入力する。

【0032】

従って、1番目の暗号化関数  $F_1$  の中間出力  $i_1$  が0であり、これに伴い、1番目の変換関数  $f_1$  の変換結果  $s_1$  が0であったとしても、1番目の変換関数  $g_1$  への入力は0にならず、変数  $v_1$  となる。

【0033】

すなわち、1番目の変換関数  $f_1$  の変換結果  $s_1$  が0であっても、1番目の変換関数  $g_1$  から出力される鍵データ  $K g_2$  は、共通鍵  $K$  が変数  $v_1$  により変換された値となって次段の暗号化関数  $F_2$  に入力される。

【0034】

以下同様に、共通鍵  $K$  は、 $(n-1)$ 番目の暗号化関数  $F_{(n-1)}$  による中間出力  $i_{n-1}$  と、 $(n-1)$ 番目の変数入力部  $V_{n-1}$  による変数  $v_{n-1}$  と、 $(n-1)$ 番目の変換関数  $f_{n-1}$ 、 $g_{n-1}$  とに基づいて、鍵データ  $K g_n$  に変換され、鍵データ  $K g_n$  として  $n$  番目の暗号化関数  $F_n$  に入力される。

【0035】

係る前段の中間出力  $i_{n-1}$  と、前段の変数  $v_{n-1}$  と、共通鍵  $K$  とから次段の鍵データ  $K g_n$  を生成する処理は、 $m$  番目の暗号化関数  $F_m$  に鍵データ  $K g_m$  を入力するまで行なわれる。

【0036】

ここで、鍵データ  $K g_2 \sim K g_m$  は、平文ブロック  $P_1 \sim P_m$  や中間結果  $i_1 \sim i_{m-1}$  とは独立に入力される変数  $v_1 \sim v_{m-1}$  に基づき、共通鍵  $K$  が変換されたものである。このため、暗復号装置は、平文ブロック  $P_1 \sim P_m$  の各ブロックを互いに同一データとして入力する暗号解読手法に攻撃されても、鍵データ  $K g_2 \sim K g_m$  を互いに異なる値に作成するので、安全性の低下を阻止することができる。

上述したように本実施形態によれば、暗号化連鎖方式において、鍵データ  $K g_2 \sim K g_m$  の生成の際に、不確定要素として変数  $v_1 \sim v_{m-1}$  を入力することに

より、鍵データ  $K_{g2} \sim K_{gm}$  を平文ブロック  $P_1 \sim P_m$  から一義的には決まらないようにしたので、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させることができる。

また、ある暗号化関数  $F_j$  に鍵データ  $K_{gj}$  として弱鍵 (weak key)、双対鍵 (dual key) 又はやや弱い鍵 (semi-week key) が入力された場合であっても、以後の暗号化関数  $F_{(j+1)} \sim F_{(m-1)}$  には弱鍵とは異なる鍵データ  $K_{g(j+1)} \sim K_{g(m-1)}$  が入力されるので、安全性を向上させることができる。

### 【0037】

#### (第2の実施形態)

図3は本発明の第2の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図である。

すなわち、本実施形態は、第1の実施形態の変形例であり、具体的には、各変数入力部  $V_1 \sim V_{m-1}$  に代えて、各変換関数  $f_1' \sim f_{m-1}'$  が、互いに異なる2以上の変換関数のいずれかとして構成されている。

### 【0038】

ここで、互いに異なる変換関数 (変換処理) とは、(a) 違う関数を用いる場合と、(b) 同じ関数を異なるビット位置に作用させる場合 (例、ビットの置換関数) と、(c) 同じ関数を異なる定数で作用させる場合 (例、加算関数で加える定数) と、のいずれかの場合又はこれらを組合せた場合が適用可能となっている。なお、第1の実施形態は、変換関数  $g_1 \sim g_{m-1}$  に対し、上記 (c) により異なる変換関数 (変換処理)  $g_1 \sim g_{m-1}$  とした例に該当する。

### 【0039】

また、各変換関数  $f_1' \sim f_{m-1}'$  は、例えば前述した変換処理 (1) ~ (8) のうち、任意の1種類以上の変換処理が使用可能となっている。

### 【0040】

なお、各変換関数  $f_1' \sim f_{m-1}'$  は、 $t$  種類の異なる関数が適用される場合、互いに隣接する任意の  $t$  個の変換関数 (例、 $f_1' \sim f_t'$ ,  $f_2' \sim f_{t+1}'$ , ...,  $f_{m-t}' \sim f_{m-1}'$ ) を互いに異なる関数とする設定の方が好ましい。

### 【0041】

以上のような構成としても、第 1 の実施形態と同様に、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させることができる。

また同様に、ある暗号化関数  $F_j$  に鍵データ  $K_{g_j}$  として弱鍵などが入力された場合でも、以後の暗号化関数  $F_{(j+1)} \sim F_{(m-1)}$  には弱鍵とは異なる鍵データ  $K_{g_{(j+1)}} \sim K_{g_{(m-1)}}$  が入力されるので、安全性を向上させることができる。

## 【 0 0 4 2 】

## (第 3 の実施形態)

図 4 は本発明の第 3 の実施形態に係る認証方式の適用された第 1 及び第 2 のエンティティ装置の構成を示す模式図であり、図 5 は各エンティティ装置に用いられる MAC 計算部の構成を代表して示す模式図である。

## 【 0 0 4 3 】

すなわち、本実施形態は、第 1 の実施形態の暗復号装置を MAC 計算部に用いた認証方式を示し、第 1 及び第 2 のエンティティ装置 1 0 A, 2 0 B を備えている。

## 【 0 0 4 4 】

ここで、第 1 のエンティティ装置 1 0 A は、メッセージ送信部 1 1 A、共通鍵記憶部 1 2 A、MAC 計算部 1 3 A 及び MAC 送信部 1 4 A を備えている。

## 【 0 0 4 5 】

メッセージ送信部 1 1 A は、メッセージ M を第 2 のエンティティ装置 2 0 B に送信する機能と、自己の MAC 計算部 1 3 A に送出する機能とをもっている。

## 【 0 0 4 6 】

共通鍵記憶部 1 2 A は、第 1 及び第 2 のエンティティ装置 1 0 A, 2 0 B の両方で共有された共通鍵 K が記憶される領域であり、MAC 計算部 1 3 A から読出可能となっている。

## 【 0 0 4 7 】

MAC 計算部 1 3 A は、共通鍵記憶部 1 2 A 内の共通鍵 K 及びメッセージ送信部 1 1 A からのメッセージ M に基づいて、第 1 の MAC 認証子 # 1 を算出（作成）する機能と、この第 1 の MAC 認証子 # 1 を MAC 送信部 1 4 A に送出する機



能とをもっている。

【 0 0 4 8 】

MAC送信部 1 4 Aは、MAC計算部 1 3 Aから送出された第 1 のMAC認証子 # 1 を第 2 のエンティティ装置 2 0 Bに送信する機能をもっている。

【 0 0 4 9 】

一方、第 2 のエンティティ装置 2 0 Bは、メッセージ受信部 2 1 B、共通鍵記憶部 2 2 B、MAC計算部 2 3 B及び照合部 2 4 Bを備えている。

メッセージ受信部 2 1 Bは、第 1 のエンティティ装置 1 0 Aから送信されたメッセージMを受信し、このメッセージMを自己のMAC計算部 2 3 Bに送出する機能をもっている。

【 0 0 5 0 】

共通鍵記憶部 2 2 Bは、第 1 及び第 2 のエンティティ装置 1 0 A、2 0 Bの両者で共有された共通鍵Kが記憶される領域であり、MAC計算部 2 3 Bから読出可能となっている。

【 0 0 5 1 】

MAC計算部 2 3 Bは、共通鍵記憶部 2 2 B内の共通鍵K及びメッセージ受信部 2 1 BからのメッセージMに基づいて、第 2 のMAC認証子 # 2 を算出（作成）する機能と、この第 2 のMAC認証子 # 2 を照合部 2 4 Bに送出する機能とをもっている。

【 0 0 5 2 】

照合部 2 4 Bは、自己のMAC計算部 2 3 Bから送出された第 2 のMAC認証子 # 2 と、第 1 のエンティティ装置 1 0 Aから受信した第 1 のMAC認証子 # 1 とを比較照合する機能と、両認証子 # 1、# 2 が一致するときに、第 1 のエンティティ装置 1 0 Aにより作成されたメッセージMが改竄されずにメッセージ受信部 2 1 Bに受信された旨を認証する機能と、両認証子 # 1、# 2 が不一致のときに、第 1 のエンティティ装置 1 0 Aにより作成されたメッセージMが改竄された旨を検出する機能とをもっている。

【 0 0 5 3 】

続いて、第 1 及び第 2 のエンティティ装置 1 0 A、2 0 Bにおける各MAC計

算部 1 3 A, 2 3 B の構成について説明する。なお、係る MAC 計算部 1 3 A, 2 3 B は、ハードウェア及び／又はソフトウェアにて実現可能なものであり、ソフトウェアにより実現される場合にはその動作を示すプログラムが予め記憶媒体からインストールされている。また、両 MAC 計算部 1 3 A, 2 3 B は互いに同一構成なので、ここでは第 1 のエンティティ装置 1 0 A 内の MAC 計算部 1 3 A を例に挙げて述べる。

## 【 0 0 5 4 】

MAC 計算部 1 3 A は、図 5 に示すように、図 1 に示した暗復号装置に対し、メッセージ M が平文データとして入力された際に、第 1 の実施形態で述べた通りに得られる m 個目（最終）の暗号文ブロック C<sub>m</sub> のうち、所定ビット位置のデータを選択するビット選択部 B<sub>s</sub> が付加された構成となっている。

## 【 0 0 5 5 】

なお、ビット選択部 B<sub>s</sub> は、選択したデータを第 1 の MAC 認証子 # 1 として MAC 送信部 1 4 A に送出する機能をもっている。また、メッセージ M 自体は、平文データに限らず、図 1 の暗復号装置と同じ又は別の暗号化装置により暗号化された暗号文データであっても良い。

## 【 0 0 5 6 】

また、以上のような第 1 及び第 2 のエンティティ装置 1 0 A, 2 0 B は、ハードウェア及び／又はソフトウェアにて実現可能なものであり、ソフトウェアにより実現される場合にはその動作を示すプログラムが予め記憶媒体からインストールされている。

## 【 0 0 5 7 】

次に、以上のように構成された第 1 及び第 2 のエンティティ装置 1 0 A, 2 0 B の動作を説明する。

第 1 のエンティティ装置 1 0 A は、メッセージ送信部 1 1 A がメッセージ M を第 2 のエンティティ装置 2 0 B に送出すると共に、このメッセージ M と共通鍵 K とに基づき、MAC 計算部 1 3 A が第 1 の MAC 認証子 # 1 を算出し、MAC 送信部 1 4 A がこの第 1 の MAC 認証子 # 1 を第 2 のエンティティ装置 2 0 B に送信する。

## 【0058】

第2のエンティティ装置20Bは、第1のエンティティ装置10AからメッセージM並びに第1のMAC認証子#1を受信すると、このメッセージMと共通鍵Kとに基づき、MAC計算部23Bが第2のMAC認証子#2を算出する。

## 【0059】

次に、照合部24Bは、この第2のMAC認証子#2と受信された第1のMAC認証子#1とを比較照合し、両認証子#1、#2が一致するときに、第1のエンティティ装置10Aにより作成されたメッセージMが改竄されずにメッセージ受信部21Bに受信された旨を認証する。また、照合部24Bは、両認証子#1、#2が不一致のときに、第1のエンティティ装置10Aにより作成されたメッセージMが改竄された旨を検出する。

## 【0060】

このような認証方式において、MAC計算部13A、23Bは、第1の実施形態と同様に、共通鍵Kを各鍵データ $K_{g2} \sim K_{gm}$ にそれぞれ変換する過程で各変数入力部 $V_1 \sim V_{m-1}$ から変数 $v_1 \sim v_{m-1}$ を入力している。従って、前述同様に、メッセージMが各ブロック毎に同一の平文（メッセージ）ブロック $P_1 \sim P_m$ となっても、鍵データ $K_{g2} \sim K_{gm}$ が互いに異なる値となるので、安全性を向上させることができる。

## 【0061】

上述したように本実施形態によれば、認証方式において、MAC認証子#1、#2を算出する際に、第1の実施形態の暗復号装置を用いたので、第1の実施形態の効果を有する認証方式を実現することができる。

## 【0062】

## (第4の実施形態)

図6は本発明の第4の実施形態に係る暗号化連鎖方式の適用されたMAC計算部の構成を示す模式図である。

すなわち、本実施形態は、第3の実施形態の変形例であり、具体的にはMAC計算部13A、23Bにおいて、各変数入力部 $V_1 \sim V_{m-1}$ に代えて、各変換関数 $f'_1 \sim f'_{m-1}$ が、互いに異なる2以上の変換関数のいずれかとして構成さ

れている。なお、図 6 は前述同様に一方の MAC 計算部 1 3 A を例に挙げて示しているが、他方の MAC 計算部 2 3 B も同様の構成となっている。

ここで、互いに異なる変換関数とは、第 2 の実施形態に述べた通りである。また、各変換関数  $f_1' \sim f_{m-1}'$  に関しても、第 2 の実施形態に述べた通りである。

以上のような構成としても、第 3 の実施形態と同様の効果を得ることができる。

#### 【 0 0 6 3 】

なお、上記各実施形態に記載した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

#### 【 0 0 6 4 】

ここで、本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD 等）、光磁気ディスク（MO 等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

#### 【 0 0 6 5 】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働している OS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等の MW（ミドルウェア）等が本実施例を実現するための各処理の一部を実行しても良い。

#### 【 0 0 6 6 】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LAN やインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

#### 【 0 0 6 7 】

また、記憶媒体は 1 つに限らず、複数の媒体から本実施例における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【 0 0 6 8 】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施例における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【 0 0 6 9 】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【 0 0 7 0 】

なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【 0 0 7 1 】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【 0 0 7 2 】

【発明の効果】

以上説明したように本発明によれば、特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上し得る暗復号装置、認証装置及び記憶媒体を提供できる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図

【図 2】

同実施形態における各変数の生成方法の一例を示すフローチャート

【図 3】

本発明の第 2 の実施形態に係る暗号化連鎖方式の適用された暗復号装置の構成を示す模式図

【図 4】

本発明の第 3 の実施形態に係る認証方式の適用された第 1 及び第 2 のエンティティ装置の構成を示す模式図

【図 5】

同実施形態における MAC 計算部の構成を代表して示す模式図

【図 6】

本発明の第 4 の実施形態に係る暗号化連鎖方式の適用された MAC 計算部の構成を示す模式図

【図 7】

従来の暗号化連鎖方式の適用された暗復号装置の構成を示す模式図

【符号の説明】

平文ブロック  $P_1 \sim P_m$

暗号化関数  $F_1 \sim F_m$

暗号文ブロック  $C_1 \sim C_m$

$K$  … 共通鍵

$K_{g2} \sim K_{gm}$  … 鍵データ

$f_1 \sim f_{m-1}$ ,  $f'_1 \sim f'_{m-1}$ ,  $g_1 \sim g_{m-1}$  … 変換関数

$i_1 \sim i_{m-1}$  … 中間出力

$v_1 \sim v_{m-1}$  … 変数

$V_1 \sim V_{m-1}$  … 変数入力部

10A, 20B … エンティティ装置

11A … メッセージ送信部

12A, 22B … 共通鍵記憶部

13A, 23B … MAC 計算部

1 4 A … M A C 送 信 部

2 1 B … メ ッ セ ー ジ 受 信 部

2 4 B … 照 合 部

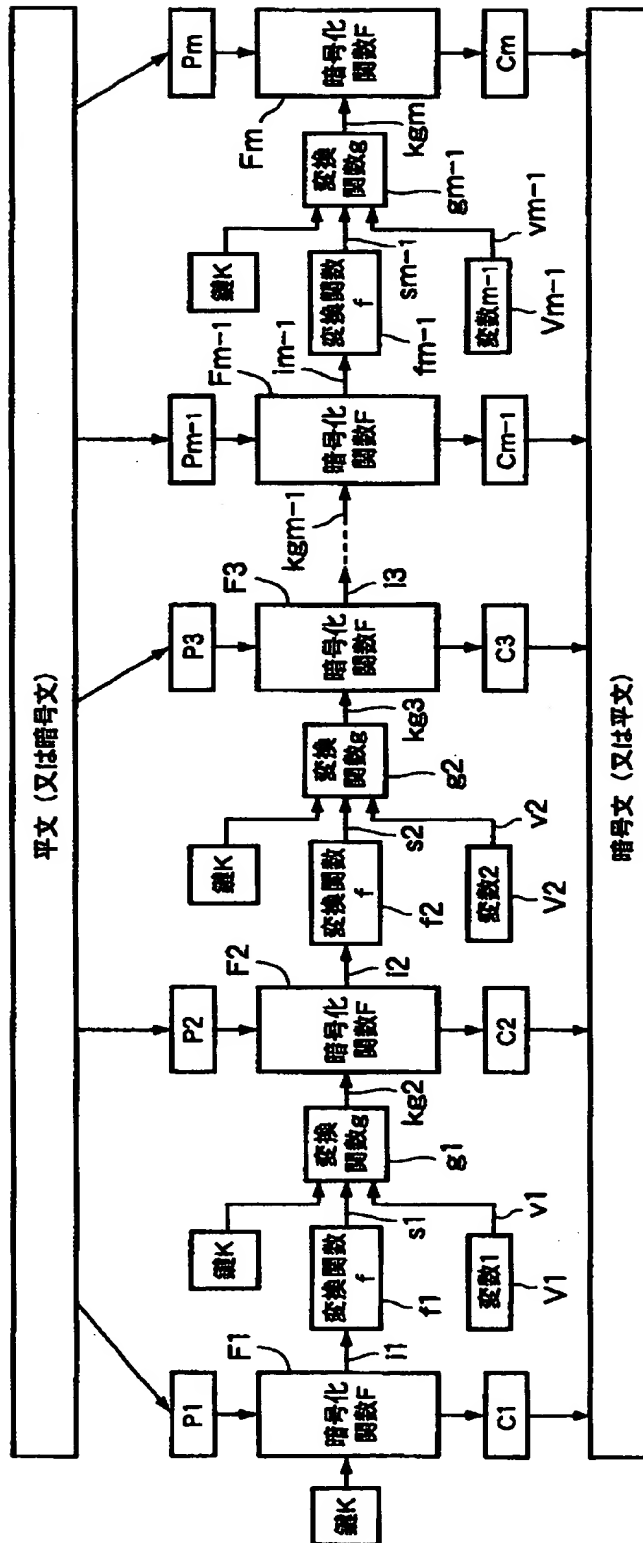
# 1 , # 2 … M A C 認 証 子

B s … ビ ッ ト 選 択 部

【書類名】

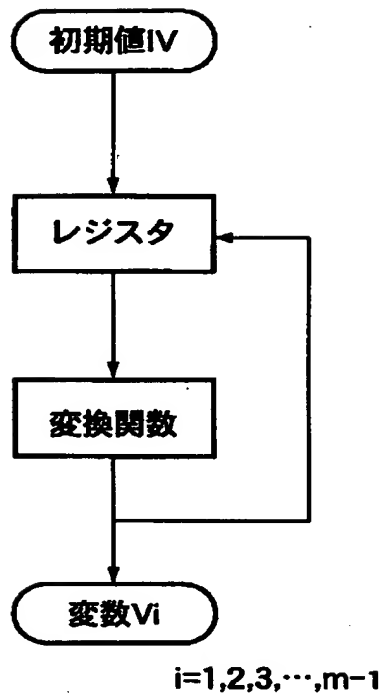
図面

【図 1】

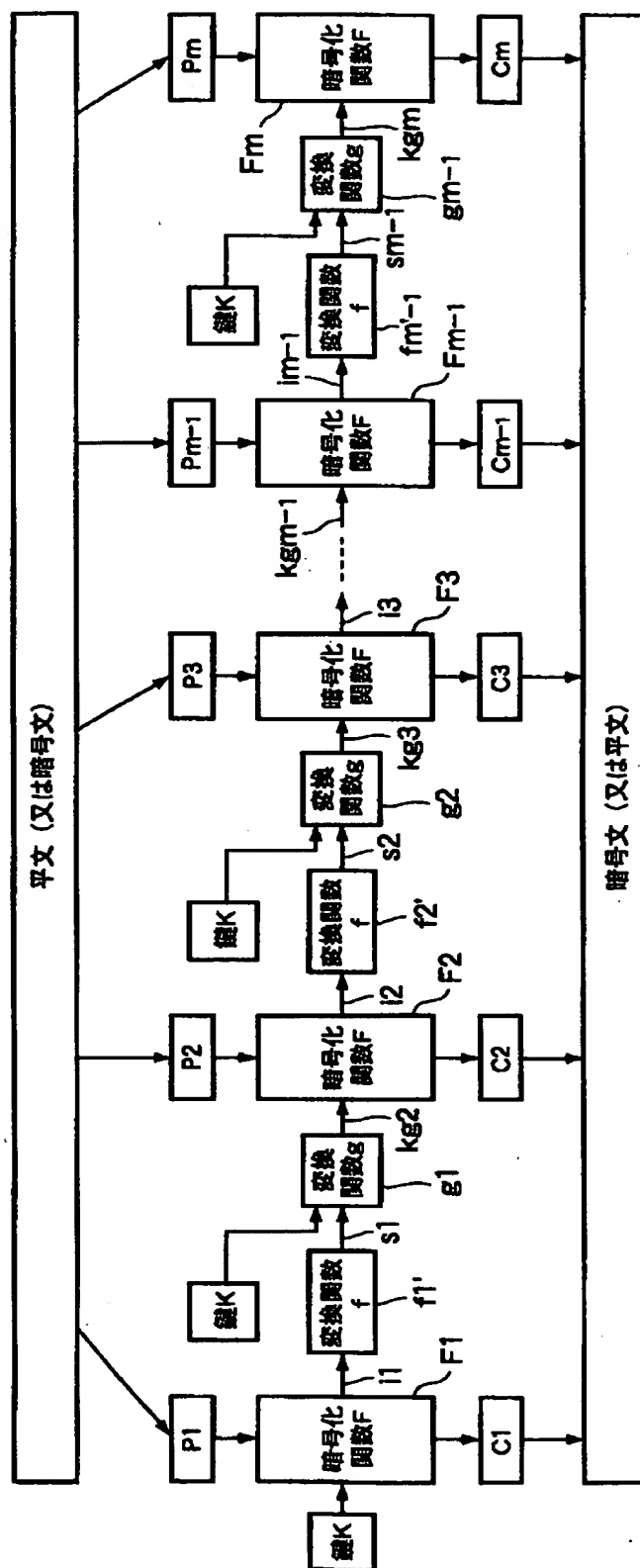




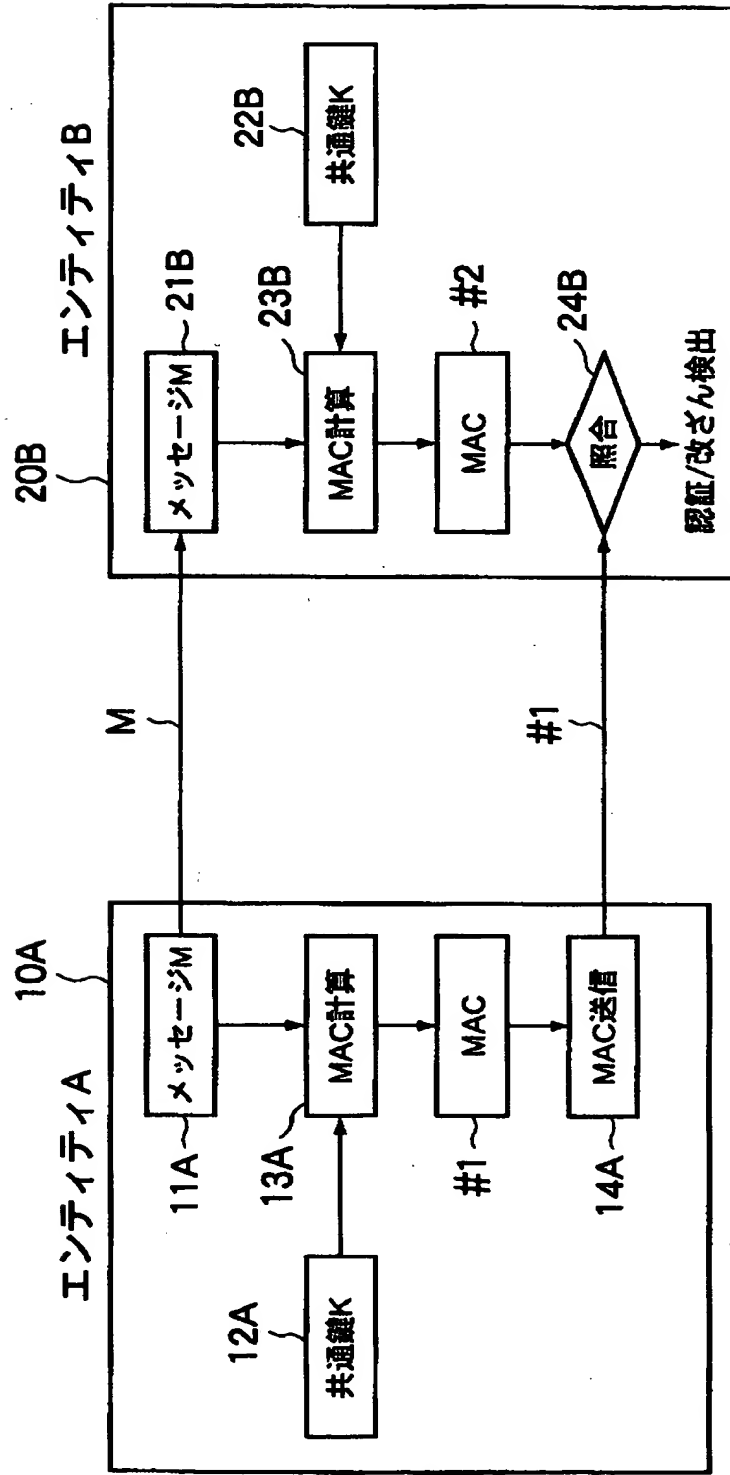
【図 2】



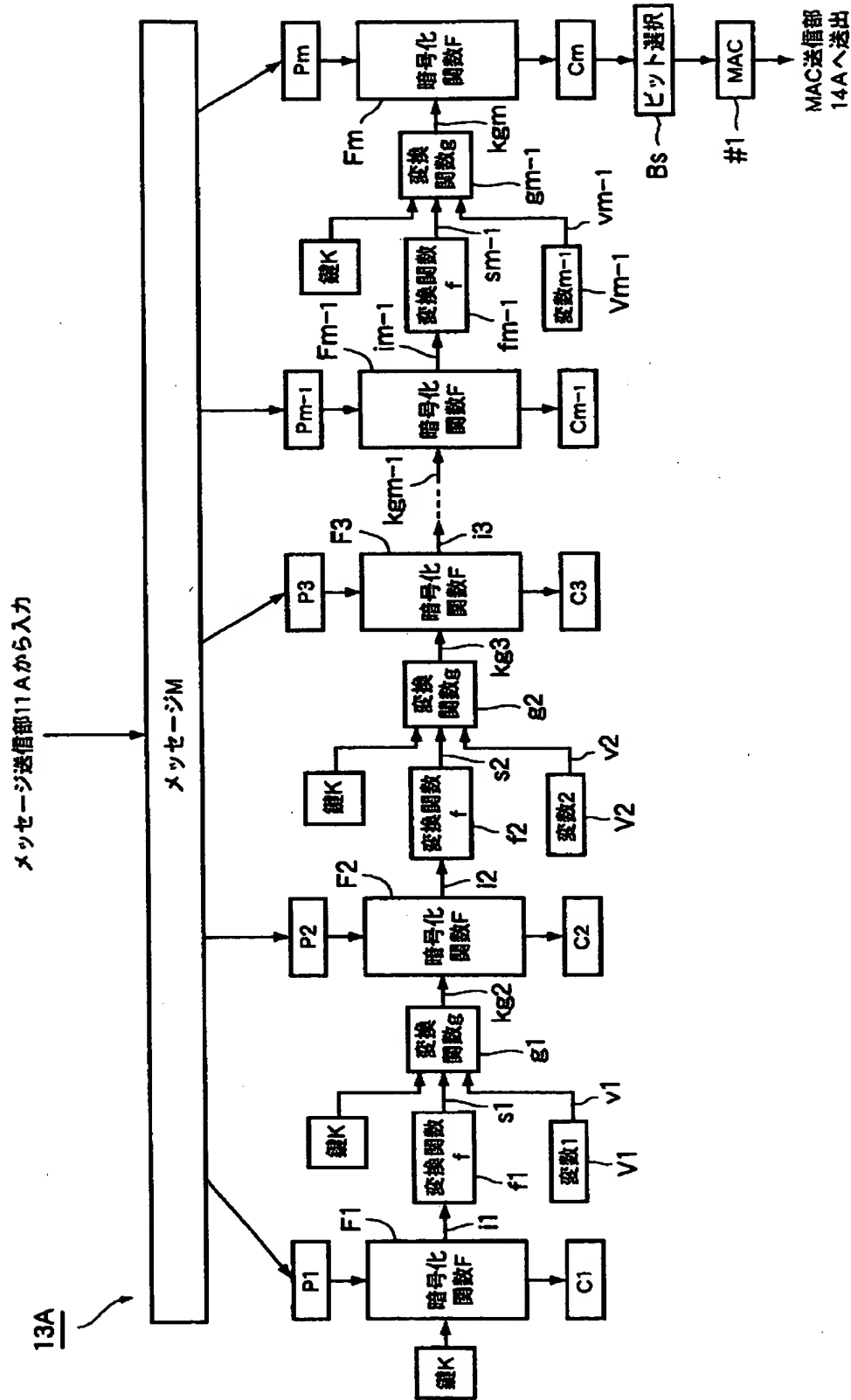
【図 3】



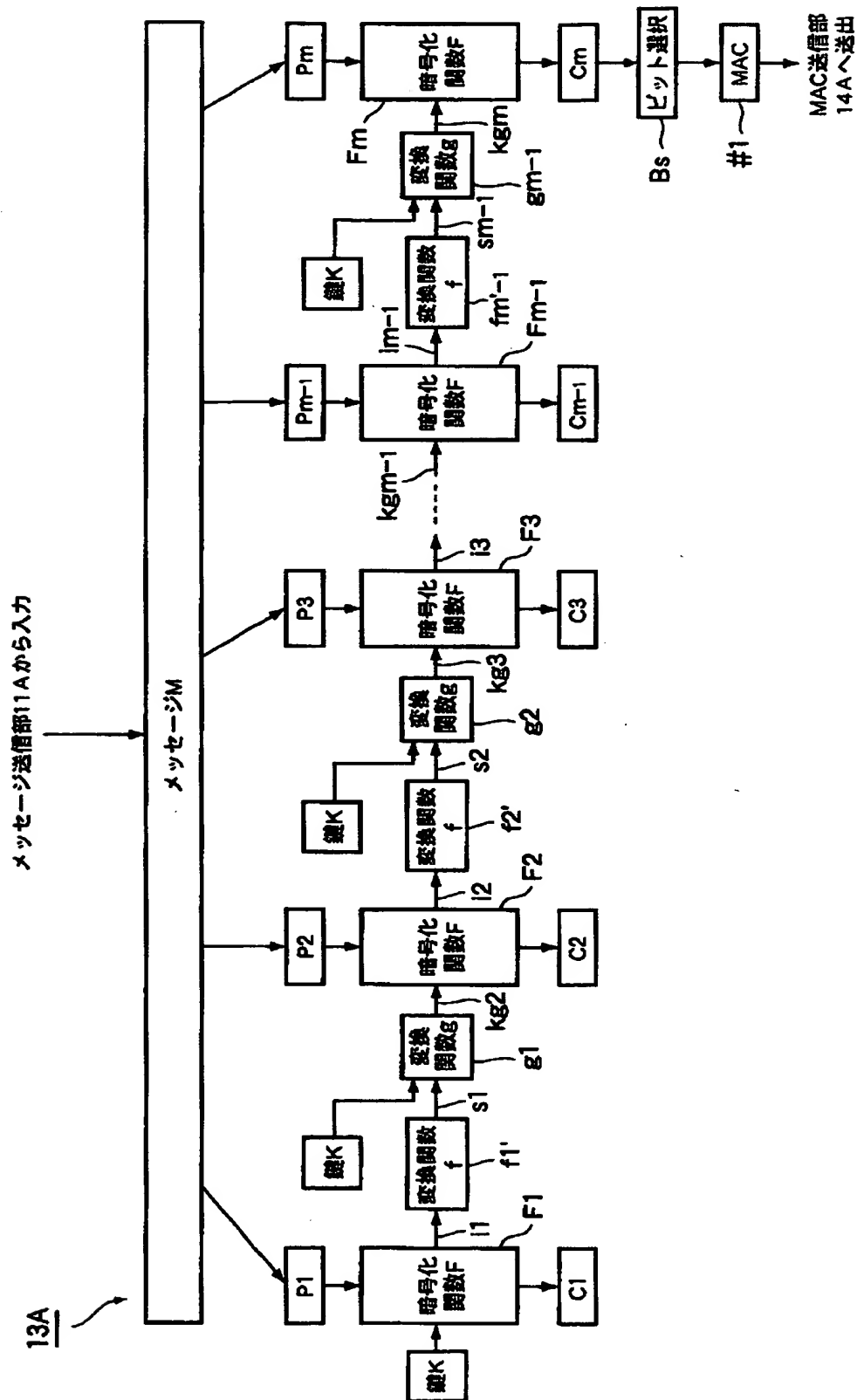
【図 4】



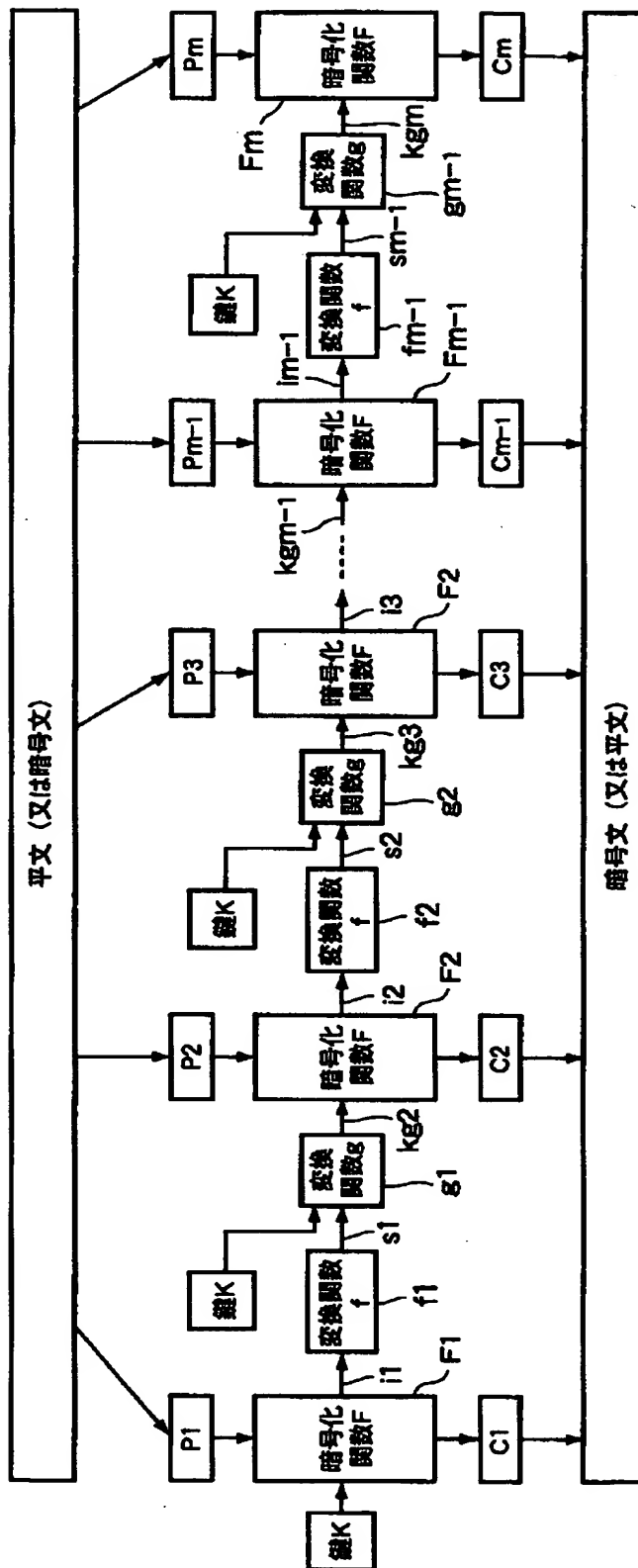
【図 5】



【图 6】



【図 7】



【書類名】                      要約書

【要約】

【課題】    特定パターンの入力の除去装置を設けずに、互いに異なる鍵データの生成を保証でき、安全性を向上させる。

【解決手段】    鍵データ  $K_{g2} \sim K_{gm}$  は、平文ブロック  $P_1 \sim P_m$  や中間結果  $i_1 \sim i_{m-1}$  とは独立に入力される変数  $v_1 \sim v_{m-1}$  に基づき、共通鍵  $K$  が変換されて作成される。このため、暗復号装置は、平文ブロック  $P_1 \sim P_m$  の各ブロックを互いに同一データとして入力する暗号解読手法に攻撃されても、鍵データ  $K_{g2} \sim K_{gm}$  を互いに異なる値に作成できる。

【選択図】    図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝